Seventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2009)
"Energy and Technology for the Americas: Education, Innovation, Technology and Practice"
June 2-5, 2009, San Cristóbal, Venezuela.

La Seguridad de la Información bajo una Perspectiva de la Madurez Organizacional

Orlando Viloria
Universidad Simón Bolívar, Caracas, Venezuela, oviloria@usb.ve

Marianella Villegas
Universidad Simón Bolívar, Caracas, Venezuela, nellavillegas@usb.ve

Walter Blanco
Universidad Simón Bolívar, Caracas, Venezuela, wblanco@usb.ve

RESUMEN

El objetivo de esta investigación fue la elaboración de un marco conceptual que describe los ciclos de aprendizaje organizacional y su relación con la gestión de la seguridad de la información en las organizaciones. La metodología fue una investigación de campo de tipo exploratoria y documental, abarcó las siguientes actividades: (a) aplicación de entrevistas y, (b) recopilación y categorización de información obtenida de investigaciones previas. Se definieron cuatro ciclos de aprendizaje; en el primer nivel destaca una actitud reactiva, en el segundo nivel la proactiva, en el tercer nivel aparecen los modelos mentales que sesgan la interpretación y la indagación de la posible solución y el cuarto nivel corresponde a la aplicación de las disciplinas de las organizaciones inteligentes para alcanzar un mayor nivel de madurez en la gestión del proceso de la seguridad de la información, asimismo representa a una organización que aprende a aprender.

Palabras Claves: seguridad de la información, aprendizaje organizacional, madurez organizacional, organizaciones inteligentes, tecnologías de la información y de la comunicación.

ABSTRACT

The objective of this research was the creation of a conceptual frame for describing organizational learning cycles and their relationship with information security management in organizations. The methodology encompassed an exploratory field and documental research. The following activities were carried out: (a) interviews and, (b) categorisation of obtained data from previous researches. Four learning cycles were defined. The first level emphasizes a reactive attitude, in the second level a proactive one, in the third level mental models appear for unleveling interpretation and research for possible solutions and, the fourth level is referred to discipline applications of smart organizations to reach a higher level of maturity in the information security management process, as well as, representing an organization that learns to learn.

Keywords: information security, organizational learning, organizational maturity, smart organizations, information and communication technologies.

1. INTRODUCIÓN

Actualmente, los planes estratégicos bajo una perspectiva de los Sistemas de Información (SI) y las Tecnologías de la Información y la Comunicación (TIC), no deben limitarse exclusivamente a la identificación de aplicaciones, información y redes que sean factores críticos de éxito para las organizaciones, entre otras cosas, también se deben abarcar otros aspectos neurálgicos inseparables de los activos informáticos, los relacionados con su seguridad. En efecto, una organización que adquiere, desarrolla y mantiene aplicaciones, bases de datos, diversas

herramientas de las TIC, si no implanta medidas de salvaguarda para proteger las vulnerabilidades inherentes a estos activos y a la información que manejan contra amenazas potenciales internas y externas, estarán expuestos a un mayor riesgo por la materialización de alguna amenaza asociada a las vulnerabilidades, en consecuencia, se generarán grandes pérdidas económicas para la institución.

En virtud de lo anteriormente expuesto, el objetivo de esta investigación es establecer un marco conceptual sobre los ciclos de aprendizaje organizacional y su relación con la seguridad de la información, en especial, la actitud asumida ante la ejecución de un ataque a los bienes informáticos. Igualmente, esta investigación tiene la finalidad de coadyuvar en la comprensión del problema, y por ende, facilitar el proceso de la planificación estratégica bajo una perspectiva de los SI y la TIC en el contexto de la seguridad de la información.

2. METODOLOGÍA

El tipo de trabajo realizado forma parte de un estudio longitudinal, pues la recolección de datos se hizo en un periodo extendido de tiempo. En efecto, esta investigación al igual que otras, está alineada con un proyecto macro de Planificación Estratégica bajo una perspectiva de los SI y las TIC Asimismo, esta investigación es un estudio de campo de tipo exploratoria, pues se revisaron una serie de trabajos relacionados con gerencia, aprendizaje organizacional, gestión tecnológica en las universidades y la seguridad de la informática, tales como: Viloria y Blanco (1999, 2000, 2001, 2004a, 2004b, 2006a; 2006b, 2006c); Blanco y Viloria (1999a; 1999b, 2001, 2006); Morales et al (2000); Morales (2004), Morales y Torrealba (2004); Torrealba (2004); Torrealba y Morales (2004, 2005), Mayorca (2007), Romero (2008) y Villegas (2008).

Villegas (2008) creó un modelo de madurez sistémico con cinco niveles de aprendizaje de la gestión de la seguridad de la información, incluyó instituciones públicas y privadas. Este estudio de campo permitió a los autores de este artículo aplicar 22 entrevistas abiertas a trabajadores del conocimiento (personal técnico y gerencial), encargados de la seguridad de la información de 11 universidades de una población de 14 ubicadas en el Distrito Capital, lo que permitió evaluar su nivel de aprendizaje bajo una perspectiva de una organización aprendiente.

Todos los trabajos de investigación referidos, así como las entrevistas realizadas, contribuyeron a establecer los bases necesarias para la identificación de variables, tendencias y estructurar el modelo propuesto, tal como lo recomiendan Hernández et al (1998). Además se identifican las relaciones entre las variables tales como los valores éticos, la actitud, la aptitud, las políticas de seguridad informática, el cooperativismo, la estructura organizacional, los procesos y las tareas, la visión y la cultura de la SIF. Estas variables ayudaron a inferir la aplicación de las disciplinas de una organización aprendiente tales como: el aprendizaje en equipo, los modelos mentales, el dominio personal, la visión compartida y el pensamiento sistémico.

3. CICLOS DE APRENDIZAJE DE LA GESTIÓN DE LA SEGURIDAD

El aprendizaje organizacional tiene muchas variantes, depende en gran medida de la madurez organizacional de las empresas para afrontar diversos problemas y adaptarse a los cambios que exige el entorno. Destacan los conceptos de aprendizaje de primer, de segundo, de tercer ciclo y por último el de las organizaciones que aprenden, este último alineado con las disciplinas de Senge (1992) y Senge et al (2004). Cada uno de estos ciclos representan un grado de madurez organizacional, los niveles superiores poseen características organizacionales, tecnológicas, gerenciales, de cultura y estructura organizacional, entre otros, más desarrolladas y consolidadas. Según el nivel de aprendizaje, las empresas pueden responder con efectividad y eficiencia ante situaciones adversas de su entorno y a factores internos que afecten su competitividad. En este mismo orden de ideas, se presenta a continuación la descripción de estos niveles de aprendizaje pero bajo el enfoque de la gestión de la seguridad de la información ante una situación de ataque a los activos informáticos.

3.1 APRENDIZAJE DE PRIMER CICLO

En este ciclo de aprendizaje, la inseguridad de la información es un problema estrictamente técnico, responsabilidad de los técnicos en computación o afín, situación señalada por Morales (2004) y Viloria y Blanco

(2006c) en sus investigaciones. En este ciclo, cuando se detecta un ataque, la situación es corregida por la implementación de una acción estructurada formulada con esa finalidad, este proceso genera un aprendizaje entre los encargados de la seguridad o la gerencia responsable. Cabe resaltar que en este nivel, las acciones preestablecidas para superar los ataques son básicas y estructuradas, lo cual no es malo para situaciones simples, ya que ayuda al desarrollo del trabajo diario (Nekane, 2000).

La Figura 1 muestra como actúa una institución de primer ciclo de aprendizaje ante un ataque a los activos informáticos. El lazo llamado nivel de inicio, es un bucle equivalente al concepto que maneja la cibernética de realimentación de procesos que busca controlar el sistema, cuando se sale de los patrones predefinidos, en este caso, un ataque a un activo informático genera cambios que afectan y alteran los objetivos de los sistemas.

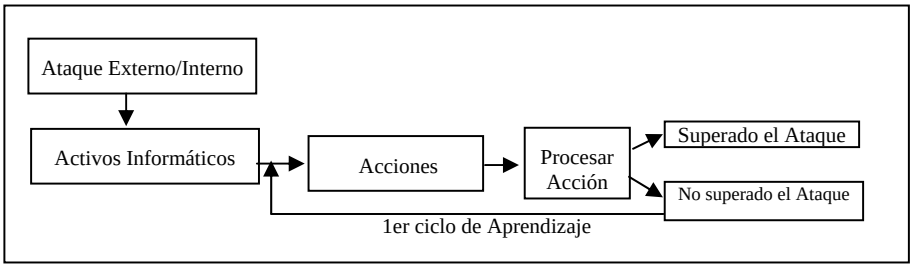

Figura 1: Aprendizaje de Primer Ciclo. Elaboración propia adaptada de Argyris y Schon (1978) citado por Nekane (2000)

En resumen, para Argyris y Schon (1978) el aprendizaje de primer ciclo se produce cuando los miembros de una organización responden a los cambios de los ambientes internos y externos de la organización, mediante la detección de errores o de desviaciones que corrigen en las salidas de los procesos, para mantener los rasgos centrales de la teoría de uso organizativa (Nekane, 2000). En tal sentido, señala Nekane que los sistemas comportan ajustes graduales de la acción organizativa para adaptarse al entorno.

Sin embargo, cuando el aprendizaje de primer ciclo no resuelve el problema, debe irse a un nivel superior de aprendizaje, el de segundo ciclo. En efecto, cuando no existe una acción estructurada para responder a un ataque a la información, la unidad encargada de la seguridad debe aumentar su nivel de aprendizaje a un segundo nivel.

3.2 APRENDIZAJE DE SEGUNDO CICLO

La organización aprende de sus errores, el aprendizaje para afrontar la inseguridad informática se manifiesta en las acciones, no se limita únicamente a corregir los daños y a superar el impacto económico causado por un ataque a los activos informáticos, sino también a reducir las vulnerabilidades. Existe conciencia de la posibilidad de desatarse un ataque básico, así como complejo, en que las acciones a ejecutar no son todas programadas. En este nivel se dan respuestas a las siguientes preguntas: ¿Por qué ocurrió este ataque?, ¿Cuáles son las vulnerabilidades?, ¿Cuál es el árbol de activos informáticos afectados? ¿En qué nos equivocamos? y ¿Cómo lo superamos?, por lo tanto existe un proceso de reflexión y de interpretación del asunto. En consecuencia, se abren nuevas y posibles acciones a seguir, se corrigen las preestablecidas si es necesario, se definen los objetivos a lograr, se va más allá del ciclo de aprendizaje 1.

Se registra la información concerniente a los ataques y vulnerabilidades y se realimenta el proceso de toma de decisiones, para evitar el desarrollo de otras amenazas y formular nuevas acciones. La Figura 2 muestra los cursos de acción en el aprendizaje de segundo ciclo, cuando ocurre un ataque a los activos informáticos de la empresa.

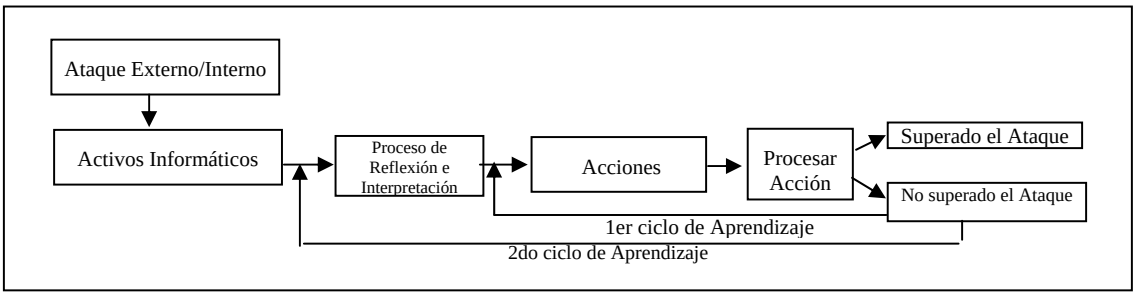

Figura 2: Aprendizaje de Segundo Ciclo

En este nivel de aprendizaje no sólo se adquiere el nivel de aprendizaje de primer y de segundo ciclo, sino que los trabajadores del conocimiento se hacen más sagaces en adquirir información, tomar decisiones, extrapolar variables, trasladar el conocimiento y adecuar el aprendizaje a distintos contextos de la seguridad (Viloria y Blanco, 2006a).

Cuando el nivel de aprendizaje de segundo ciclo no es efectivo para la solución de problemas, hay que subir otro peldaño en el aprendizaje, que corresponde al aprendizaje de tercer ciclo, se deben revisar los modelos mentales existentes (Viloria y Blanco, 2006a).

3.3 APRENDIZAJE DE TERCER CICLO

Cuando la solución no está en la instrumentación de cursos de acción ni en el proceso de reflexión e interpretación, los encargados de la seguridad y la gerencia deben ir más allá y revisar los modelos mentales existentes, pues el problema puede estar allí y afecta la efectividad de las estrategias (ver Figura 3). En efecto, deben investigarse cuáles son los modelos mentales que condicionan las interpretaciones de los trabajadores del conocimiento y tienen un efecto directo en las decisiones destinadas a resolver problemas (Viloria y Blanco, 2006a). Al respecto Nekane (2000) señala: “en el aprendizaje 3, se comienza a examinar cómo estos factores (modelos mentales) crean predisposición para interpretar al mundo en formas que pueden generar insatisfacción y estrés”.

En una organización tradicional los modelos mentales constituyen la base de la cosmovisión, de la interpretación del mundo, conducen a los gerentes a tomar decisiones sesgadas, sobre todo cuando no están enmarcados en la disciplina de las organizaciones inteligentes (Senge, 1992). Igualmente, los individuos alineados con sus modelos, asumen que todos tienen los mismos paradigmas, los llevan por caminos que conducen a creencias erróneas sobre el problema de la inseguridad de la información. A partir de éstos, “se estructuran los datos, la información y el conocimiento dando lugar a las teorías y modelos que constituirán los mapas con los que se interpreta y moldea la realidad, o habría que decir su realidad” (Ragno, 2002). “La incapacidad para apreciar los modelos mentales conspira contra los esfuerzos para alentar el pensamiento sistémico” (Senge, 1992). En consecuencia los responsables de la seguridad no pueden analizar los problemas bajo una perspectiva sistémica, sino con una visión parcial de la realidad.

Por lo tanto, en este nivel afloran estos modelos, y son sometidos a una rigurosa revisión e indagación por parte de los equipos encargados de la seguridad, en este proceso son sustituidos por otros compartidos, alineados a la disciplina de las organizaciones inteligentes. Es importante señalar la presencia de los equipos de seguridad, de desarrollo de sistemas y de soporte técnico bien constituidos y críticos para el proceso de aprendizaje de tercer nivel, además la comunicación entre ellos es vital para responder con efectividad ante los ataques.

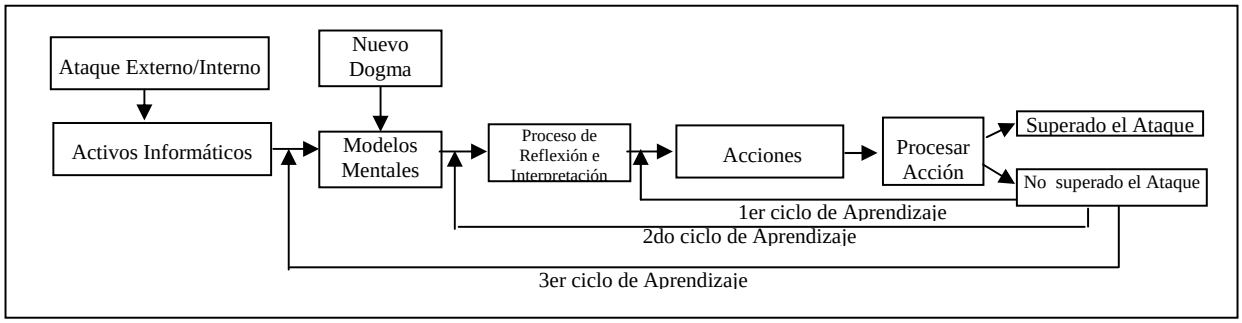

Figura 3: Aprendizaje de Tercer Ciclo

Por un lado, la disciplina de los modelos mentales se encuentra entre los nuevos dogmas de una organización inteligente (Senge et al, 2004), por ello aparece en la Figura 3. Por otro lado, en este ciclo de aprendizaje, los trabajadores encargados de la seguridad requieren de más compromiso, de mejorar su actitud y aptitud, pero en un proceso permanente de aprendizaje, que nunca termina, ya que nuevos SI y TIC son implantados continuamente y generan nuevas formas de ataque, asociadas a las innovaciones. Sin embargo, profundizar el aprendizaje es alcanzar la visión personal y compartida, así como desarrollar el dominio personal. En consecuencia, todavía se requiere de un mayor nivel de aprendizaje y la consolidación de las otras disciplinas de las organizaciones inteligentes.

3.4 LA ORGANIZACIÓN APRENDIENTE

En este nivel, el departamento de seguridad llega a un máximo estado de aprendizaje, están presentes las cinco disciplinas de las organizaciones inteligentes: los modelos mentales, el dominio personal, la visión compartida, el aprendizaje en equipo y el pensamiento sistémico, éste corresponde a la quinta disciplina que es la relación sistémica entre las cuatro primeras (Senge, 1992; Senge et al, 2004). Las organizaciones que aprenden tienen institucionalizados procesos de reflexión y aprendizaje en la planificación y evaluación de sus acciones, adquiriendo una nueva competencia; lo que implica transformar los modelos mentales vigentes, así como generar visiones compartidas. La operacionalización y desarrollo de estas disciplinas permitirá responder con inteligencia a los ataques hacia los activos informáticos. La institución que alcance este nivel, estará por encima de aquéllas que actúan bajo un esquema de primer, segundo o tercer ciclo de aprendizaje, será una organización que aprenderá a aprender (Viloria y Blanco, 2006a).

En este nivel aparece la figura del departamento, unidad administrativa o equipos de trabajadores del conocimiento cuya misión es velar por la seguridad de los bienes informáticos, tanto lógica como física, ellos se diferenciarán de sus homólogos de otras organizaciones menos maduras con un ciclo de aprendizaje más bajo, por el dominio de las cinco disciplinas de las organizaciones inteligentes. La Figura 4 muestra la influencia de las cinco disciplinas en el proceso de responder a un ataque.

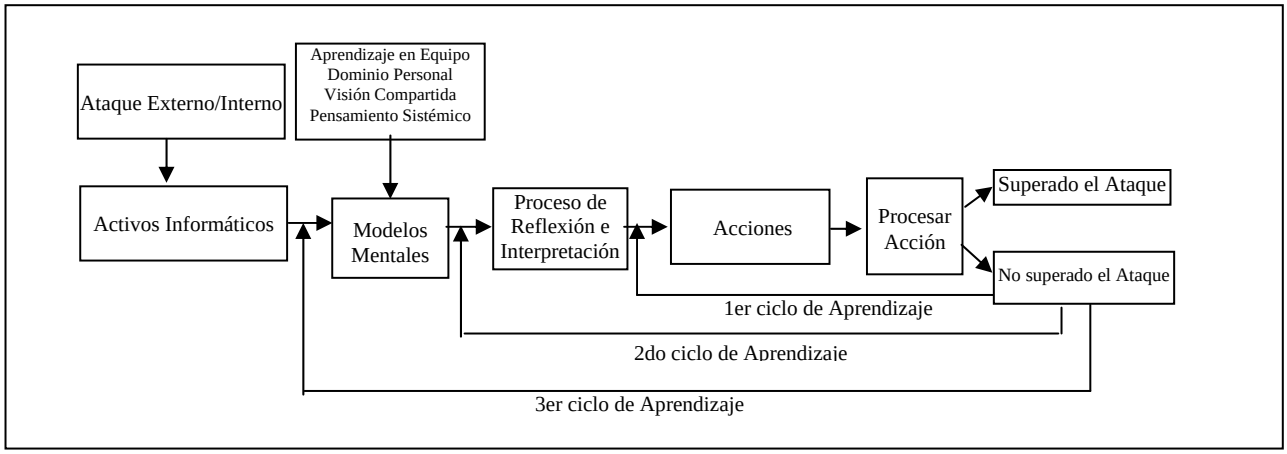

Figura 4: La Seguridad en la Organización Aprendiente

En el cuarto ciclo, los modelos mentales de las disciplinas de las organizaciones aprendientes están conectados a las otras disciplinas (ver Figura 4), todas relacionadas sistémicamente. El trabajo en equipo madura y sus integrantes crecen con rapidez, la inteligencia del grupo supera la inteligencia individual de los miembros del equipo, en efecto, generan sinergia. La diferencia de este ciclo de aprendizaje con el tercer nivel es la consolidación y el desarrollo de las disciplinas de las organizaciones inteligentes en el ambiente del departamento o unidad equivalente de seguridad. Lo importante es que la respuesta ante un ataque sea eficiente y efectiva, y sobretodo, con mucha experticia técnica por la presencia del dominio personal. Cabe destacar que este nivel es una extensión del tercer ciclo, ya que mejora las condiciones organizacionales y el aprendizaje en equipo, pues permite a la organización responder al surgimiento de nuevas vulnerabilidades asociadas a la innovación tecnológica. En este ciclo, la unidad encargada de la seguridad de la información, trabaja con base en la experticia técnica personal y del equipo, desarrolla su potencial creativo alentado por la gerencia del departamento, trabaja bajo una misma visión y siempre con un enfoque sistémico. Está en capacidad de recopilar, categorizar y procesar datos para realizar análisis y gestión de riesgo con el objetivo de reducir las vulnerabilidades a los ataques informáticos así como realizar, difundir y hacer cumplir políticas de seguridad informática (Amendolia. y Cendagorta, 2004) en el contexto de la quinta disciplina

4. CONCLUSIONES

Una organización en el primer ciclo de aprendizaje nunca podrá responder ante un ataque complejo, incluso algunos ataques no serán ni siquiera detectados, y las consecuencias de los mismos tendrán un alto costo para la organización.

En el segundo ciclo de aprendizaje, los trabajadores del conocimiento responsables de la seguridad informática tienen una actitud proactiva ante situaciones irregulares que desequilibran y disparan la entropía en el departamento o en los equipos de seguridad, tienen las destrezas para formular estrategias y superar muchos de los ataques a los bienes informáticos.

El tercer ciclo de aprendizaje supera las expectativas con respecto a su nivel anterior, reduce el riesgo de que se materialice una amenaza, aumenta las posibilidades de éxito por la afloración de los modelos mentales que sesgan las decisiones y generan estrategias equivocadas que no permiten superar situaciones complejas de ataque.

El contexto organizacional de la seguridad en una organización aprendiente es una amplificación del tercer ciclo de aprendizaje, con la diferencia de que están arraigadas las disciplinas de las organizaciones inteligentes en los equipos cuyo rol es velar por superar situaciones de inseguridad. Estos grupos generan un conocimiento que les permite responder con eficiencia y efectividad a eventos que trastocan la estabilidad de los SI y las TIC.

REFERENCIAS

Amendolia D. y Cendagorta J. (2004). Políticas de Seguridad Informáticas. http://www.criptored.upm.es/guiateoria/gt_m148q.htm, 01/20/09.

Argyris, C. y Schon, (1978). *Organizational Learning: A Theory of Action Perspective*. Massachusetts, Addison Wesley.

Blanco, W. y Viloria, O. (1999a). *Análisis y Diagnóstico de la Situación Actual en Sistemas y Tecnologías de la Información y una Propuesta de Acciones estratégicas para la USB – Sede del Litoral*. Trabajo de ascenso para optar a la categoría de Asociado. Universidad Simón Bolívar. Venezuela.

Blanco, W. y Viloria, O. (1999b). "Aspectos Organizacionales a Considerar en el Desarrollo de un Sistema de Información Universitario para la Universidad Simón Bolívar Sede del Litoral". *Revista VI de Investigación*, Vol. 6, Número Único, p. 65-84. Caracas. Venezuela.

Blanco, W. y Viloria, O. (2001). "Propuesta de un Plan Estratégico de Desarrollo de Sistemas y Tecnologías de la Información para el Decanato de Estudios Tecnológicos de la USB Litoral (Fase II)". *Revista Perfiles*. Año 22, N°2, p. 53-73. Caracas. Venezuela.

Blanco W. y Viloria, O. (2006). "Modelos mentales de la USB y su influencia en el retorno al Litoral Central". *Revista Venezolana de Análisis de Coyuntura*. Vol. 12, Numero 2. Caracas. Venezuela.

Hernández, R.; Fernández, C. y Baptista, P. (1998): *Metodología de la Investigación*. Edit. MacGraw-Hill. México.

Mayorca, R. (2007). "Dimensión del Aprendizaje Organizacional de la Universidad Venezolana". Trabajo Especial de Grado de Magíster en Gerencia Empresarial. Universidad Simón Bolívar. Caracas. Venezuela.

Morales, M. (2004). "Intranet Académica: Modelo del Sistema de Seguridad para un Servicio de Publicaciones". Trabajo de Grado de Magíster en Ciencias de la Computación: Mención Comunicación y Redes. Facultad de Ciencias, Escuela de Computación de la Universidad Central de Venezuela, Caracas, Venezuela.

Morales M., Viloria O., Torrealba M. & Isern G.(2000). "Intranet Service Security System Design: Venezuelan Public Universities, a Case Study". *4th World Multiconference on Systemics, Cybernetics and Informatics (SCI 2000) Proceeding Comunications Systems and Networks*, Volumen IV. Pp 510-514. Orlando, Florida, USA.

Morales M. y Torrealba M. (2004). "Desarrollo de un Modelo de Seguridad para Publicaciones Académicas en el Web mediante UML". *Memorias de la III Conferencia Iberoamericana en Sistemas, Cibernética e Informática CISCI 2004*, Orlando, Florida, EUA.

Nekane, A. (2000). "Un estudio desde la Perspectiva de Cambio. Implicaciones estratégicas y organizativas". Tesis Doctoral. Universidad de Deusto. San Sebastián. España.

Ragno, L.(2002). Nuevas Metáforas de la Gestión de Organizaciones, Monterrey. www.ruv.itesm.mx/cgi-bin/pgit/TWiki/bin/view/Madison2/SistemasAprendientes, 10/18/08. México.

Romero, B. (2008). "Valoración de Activos en el Riesgo para Aplicaciones Web Universitarias. Estudio de Caso: USB". Tesis para optar al grado de Magíster en Ingeniería de Sistemas. Mención Sistemas de Información. Coordinación de Postgrado de Ingeniería de Sistemas. Universidad Simón Bolívar. Caracas. Venezuela.

Senge, P. (1992). *La Quinta Disciplina.* Edit. Granica, Barcelona, España.

Senge, P., Ross R., Smith B., Roberts Ch. y Kleiner A. (2004). *La Quinta Disciplina en la Práctica.* Ediciones. Granica, Buenos Aires Argentina.

Torrealba, M. (2004). "Desarrollo de un Sistema de Apoyo de Redes TCP/IP que Detecta Ataques que se realizan a la Seguridad a través de la Técnica de Covert Channels Sobre ICMP". Tesis para optar al grado de Magíster en Ciencias de la Computación. Mención Comunicación y Redes. Facultad de Ciencias. Escuela de Computación de la Universidad Central de Venezuela. Caracas. Venezuela.

Torrealba, M. y Morales, M. (2004*).* "Modelo de un IDS para Proteger Sistemas del Tráfico ICMP: Caso del Ataque Loki". *Memorias de la III Conferencia Iberoamericana en Sistemas, Cibernética e Informática CISCI 2004*, Orlando, Florida, EUA.

Torrealba, M. y Morales, M. (2005). "La Quinta Disciplina como Alternativa Estratégica en la Administración de la Seguridad Telemática". *LIV Convención Anual de la ASOVAC*. Universidad Central de Venezuela. Facultad de Ciencias. Caracas. Venezuela.

Villegas, M. (2008). "Modelo de Madurez para la Gestión de la Seguridad Informática en las Organizaciones". Trabajo de Grado de Magíster en Ingeniería de Sistemas. Mención Sistemas de Información. Coordinación de Postgrado de Ingeniería de Sistemas. Universidad Simón Bolívar. Caracas. Venezuela.

Viloria, O. y Blanco, W. (1999). "Propuesta de un Plan Estratégico para un Departamento de Computación". *Lumen XXI*, VII, N° 2, Universidad Rómulo Gallegos, p. 118-138. San Juan de Los Morros. Estado Guárico. Venezuela.

Viloria, O. y Blanco, W. (2000). "Evaluación de la Calidad del Servicio del Departamento de Admisión y Control de Estudios de la Universidad Simón Bolívar - Sede del Litoral bajo una perspectiva de Sistemas y Tecnologías de la Información". *Revista Perfiles*, año 21, N° 1. USB. Caracas. Venezuela.

Viloria, O. y Blanco, W. (2001). "Análisis de la Situación Actual del Decanato de Estudios Tecnológicos de la Universidad Simón Bolívar - Sede del Litoral desde una Perspectiva de Sistemas y Tecnologías de la Información (Fase I)". *Revista Perfiles*. Año 22, N° 1. Caracas. Venezuela.

Viloria, O. y Blanco, W. (2004a). "Aspectos a considerar en una Metodología de Planificación Estratégica de Sistemas y Tecnologías de la Información para el Contexto Universitario Venezolano". *Memorias de la III Conferencia Iberoamericana en Sistemas, Cibernética e Informática CISCI 2004*. Orlando, Florida. EUA.

Viloria, O. y Blanco, W. (2004b). "Análisis Sistémico del Proceso DDD Bajo una Perspectiva de las Cinco Disciplinas de las Organizaciones Inteligentes: Caso USB – NUL". *Revista Iberoamericana de Sistemas, Informática y Cibernética.* (ISSN: 1690-8627), Vol. 2, Nº 1. Florida. E.U.A. Disponible: http://www.iiisci.org/Journal/riSCI/ [Consulta: 2005, Noviembre 11]

Viloria, O. y Blanco W. (2006a). "Factores que Bloquean la Aplicación de las Disciplinas de las Organizaciones Inteligentes en el Núcleo del Litoral de la Universidad Simón Bolívar". *Revista Espacios*. Vol. 27, Nº 3. Caracas. Venezuela.

Viloria, O. y Blanco W. (2006b). **"**El Sistema DDD y el Proceso de Estimación de la Oferta Académica Bajo Una Perspectiva de la Teoría del Caos: Caso USB-NUL". Revista Perfiles. Número Único, año 27. Caracas. Venezuela.

Viloria, O. y Blanco, W. (2006c). "Propuesta Metodológica de Planificación Estratégica de los Sistemas de Información y las TIC bajo el Contexto de las Organizaciones Inteligentes para el Sector Universitario". Trabajo de Ascenso para optar a la categoría de Titular. Universidad Simón Bolívar. Venezuela.

Autorización y Renuncia

Los autores authorizan a LACCEI para publicar el escrito en los procedimientos de la conferencia. LACCEI o los editors no son responsables ni por el contenido ni por las implicaciones de lo que esta expresado en el escrito

Authorization and Disclaimer

Authors authorize LACCEI to publish the paper in the conference proceedings. Neither LACCEI nor the editors are responsible either for the content or for the implications of what is expressed in the paper